Pergamon

Computers Math. Applic. Vol. 29, No. 2, pp. 1–12, 1995

0898-1221/95 $7.00 + 0.00

0898-1221(94)00212-6

The Shortest Single Axioms for Groups of Exponent 4

K. KUNEN
Computer Sciences Department, University of Wisconsin
Madison, WI 53706, U.S.A.
kunen@cs.wisc.edu

Abstract—We study equations of the form $(\alpha = x)$, which are single axioms for groups of exponent 4, where α is a term in product only. Every such α must have at least nine variable occurrences, and there are exactly three such α of this size, up to variable renaming and mirroring. These terms were found by an exhaustive search through all terms of this form. Automated techniques were used in two ways: to eliminate many α by verifying that $(\alpha = x)$ is true in some nongroup, and to verify that the group axioms do indeed follow from the successful $(\alpha = x)$. We also present an improvement on Neumann's scheme for single axioms for varieties of groups.

Keywords—Group, Paramodulation, Resolution, Exponent.

1. INTRODUCTION

In this paper, we shall prove a number of theorems on single axioms for groups. The proofs utilize a computer, employed as what L. Wos has called a "reasoning assistant." That is, as far as is possible, we proceed by "standard" mathematical reasoning. However, at some point, the proofs require computer assistance. This assistance is of two separate sorts. First, we make use of the automated reasoning program OTTER, developed by McCune [1,2], to verify some logical inferences. Second, we use more conventional programming techniques to search for models for various axioms.

We begin by emphasizing the mathematics, and call in the computer when it is needed. If $n \geq 1$ is an integer, a *group of exponent* n is a group in which x^n is the identity for all elements x. We study equations of the form $(\alpha = x)$ which are single axioms for groups of exponent n, where α is a term in product only. Note that in our definition of "exponent n," we do not require that n is the smallest exponent; hence, for example, every group of exponent 2 is also a group of exponent 4. The class of groups of exponent "precisely 4" (that is, also satisfying $\exists y(y^2 \neq e)$) cannot be axiomatized by any set of equations.

First, some notation on terms. We shall use the binary function symbol t to denote the group product. We shall also sometimes use standard infix algebraic notation as an abbreviation, with products associating to the right. Thus, for example, $x \cdot y \cdot z$ and xyz both abbreviate the term $t(x, t(y, z))$. We use exponentiation as a further abbreviation, with x^1 abbreviating x, and x^{n+1} abbreviating $x \cdot x^n$. Let $RA(\alpha)$ result from associating all products in α to the right; thus, for example, $RA(t(t(x, y), t(z, u)))$ is $t(x, t(y, t(z, u)))$, which is the same as $xyzu$ by our conventions on algebraic notation.

Because of the finite exponent, we can express all the group axioms in terms of product only. Thus, we say that a *group of exponent* n is a model for the following set of three axioms:

This research was supported by NSF Grant DMS-9100665.

G1. $t(x,t(y,z)) = t(t(x,y),z)$,
G2. $x^n = y^n$,
G3. $x \cdot y^n = x$.

The variables x, y, z are understood to be universally quantified. For $n = 1$, G2 reduces to $x = y$, so the only model is the trivial 1-element group. For $n > 1$, G2 says that x^n is some constant, e. Then, by G2, we have $x^n = e$, and, since x^n is really the term $x \cdot x^{n-1}$, we have a right inverse, x^{n-1}, for each x. G3 says that e is a right identity, so G1,G2,G3 are equivalent to the usual statement of the axioms for groups of exponent n.

If α is a term constructed from t and variables, then we say that the equation $(\alpha = x)$ is a *single axiom* for groups of exponent n iff $(\alpha = x)$ is valid in all groups of exponent n and every model for $(\alpha = x)$ satisfies G1,G2,G3. Neumann [3] proved that such α exist. Actually, he found a general scheme for single axioms for any variety of groups, but the single axioms for exponent n groups produced as instances of this scheme are quite large, and it is natural to ask whether simpler ones exist.

Let $V(\alpha)$ be the number of variable occurrences in α. Since we have only the one function symbol, t, we shall take $V(\alpha)$ as a measure of the size of α, which will then have $V(\alpha) - 1$ occurrences of t. In Section 3, we shall prove the following result, which establishes a minimum size for such α:

THEOREM 1.1. *Suppose $(\alpha = x)$ is a single axiom for groups of exponent $n > 1$. Then*

a. *$V(\alpha) = kn + 1$ for some $k \geq 2$.*
b. *If $V(\alpha) = 2n + 1$, and $n > 3$ is even, then $RA(\alpha)$ is of the form $y^n x z^n$, where y, z are two distinct variables other than x.*

In particular, then, $V(\alpha) \geq 2n + 1$. The single axioms from Neumann's scheme have $V(\alpha) = n^4 - 2n^2 + n + 1$ (see Section 6), which is quite a bit larger than this minimum. However, it is known that for $n = 2$ (see [4]) and for n odd (see [5]), there are single axioms with $V(\alpha) = 2n+1$. The situation for even $n > 2$ remained open.

In this paper, we settle the question for $n = 4$ by showing that there are single axioms of minimal size $(V(\alpha) = 9)$:

THEOREM 1.2. *Each of the following is a single axiom for groups of exponent 4:*

A0. $t(y,t(t(y,t(t(y,y),t(x,z))),t(z,t(z,z)))) = x$,
A1. $t(t(t(y,y),y),t(t(t(y,t(x,z)),t(z,z)),z)) = x$,
A2. $t(t(y,t(t(t(t(y,y),y),t(x,z)),z)),t(z,z)) = x$.

This theorem may be verified with OTTER, along with a few tricks, as described in Section 4.

We found these axioms by doing an exhaustive search through all possible candidates with 9 variable occurrences. One curious outcome of the search is that, up to variable renaming and mirror symmetry, A0, A1, and A2 are the only single axioms of this size. By *mirroring*, we mean reversing the order of t; formally, let $\mathcal{M}(t(\alpha,\beta))$ be $t(\mathcal{M}(\beta),\mathcal{M}(\alpha))$, and let $\mathcal{M}(V)$ be V if V is a variable. Then $(\alpha = x)$ is a single group axiom iff $(\mathcal{M}(\alpha) = x)$ is. This mirror symmetry was also exploited by McCune [6] and McCune and Wos [5]; it cuts the search space in half. A *renaming* of an equation is an equation obtained by changing the names of some (possibly all, or possibly none) of the variables. The statement that A0,A1,A2 are the only single axioms of this size can be stated formally as follows:

THEOREM 1.3. *Suppose that $(\alpha = x)$ is a single axiom for groups of exponent 4 and $V(\alpha) = 9$. Then some renaming of $(\alpha = x)$ or of $(\mathcal{M}(\alpha) = x)$ is one of* A0,A1,A2.

In contrast, McCune and Wos [5] found 14 different single axioms of minimal size for exponent 5 groups, and we do not know whether there are any more. This indicates that single axioms for even exponent groups are rarer than those for odd exponent groups, and it is not clear whether there are small single axioms for groups of any even exponent greater than 4.

We remark that exponent 2 is a special case, since all groups of exponent 2, the *Boolean* groups, are Abelian, and short single axioms for Boolean groups have a special form; see the discussion in Section 3 following the proof of Theorem 1.1.

In Section 2, we describe three classes of nongroup countermodels that were useful in defeating large numbers of α in our exhaustive search. In Section 5, we describe the details of the search itself, and the proof of Theorem 1.3. All the candidates except for the three successful single axioms are true in one of the classes of models described in Section 2.

There is a sense in which our three single axioms, `A0`,`A1`,`A2`, are all variants of each other. This is explained at the end of Section 5.

In Section 6, we explain how to use OTTER to verify Neumann's scheme, as well as a somewhat simpler scheme.

2. SUMMARY OF COUNTERMODELS

We describe three classes of nongroup models which can be used to eliminate many candidates for single axioms. We also comment on how these models can be used in an automated search. The first two classes were also used in [7], but there are some changes from [7], which considered terms using inverse as well as product. The third is an application of the Knuth-Bendix [8] method.

The first result is taken directly from [7] and applies more generally to terms using inverse (i) and identity (e) as well as product.

THEOREM 2.1. *There is a finite structure $\mathcal{G} = (G; t_G, i_G, e_G)$ for the language of group theory such that*

1. *t_G is not associative (so $\mathcal{G}$ is not a group).*
2. *If $(\alpha = \beta)$ is any equation valid in all Boolean groups, where α, β are built from t, i, e, x, y, then $(\alpha = \beta)$ is valid in $\mathcal{G}$.*

The proof in [7] shows how to build a model by adjoining one element to a Steiner triple system.

If n is even, then any Boolean group has exponent n, so this theorem implies that $(\alpha = x)$ cannot be a single axiom for groups of exponent n unless α has at least 3 distinct variables. Theorem 1.1 places much more stringent requirements on the α we consider. However, Theorem 2.1 will still be very useful in eliminating many α that conform to the requirements of Theorem 1.1, such as

$$((yy)(yy)) \cdot ((((xz)z)z)z) = x,$$

which cannot be a single axiom for groups of exponent 4 because it is derivable from the set of all 2-variable equations valid in all Boolean groups.

One might eliminate candidates by checking their validity in a $\mathcal{G}$ satisfying Theorem 2.1; such a model, of size 10, is described in [7]. However, in practice, such a check would be rather slow. We found it quicker to use a purely syntactic approach. We treated x, y, z as constants and deleted all α which can be reduced to x by demodulating with

$$t(e,\delta) = \delta, \qquad t(\delta,e) = \delta, \qquad t(\delta 1,\delta 2) = e,$$
$$t(t(\delta 1,\tau),\delta 2) = \tau, \qquad t(t(\tau,\delta 1),\delta 2) = \tau, \qquad t(\delta 2,t(\delta 1,\tau)) = \tau, \qquad t(\delta 2,t(\tau,\delta 1)) = \tau,$$

where τ, δ are any terms, and $\delta 1, \delta 2$ are any terms that can be reduced to each other by just applying commutativity of t. We accomplished this demodulation by a simple Prolog program, which reads a file of candidate α and eliminates the ones which reduce to x. One could also use OTTER for this.

Another class of models, the *ring models*, eliminates a large number of potential single axioms. Suppose that $\mathcal{A} = (A;\ +, \cdot, 0, 1)$ is a ring with unity. If we fix $h, k \in A$, we let $\mathcal{R}(h, k, \mathcal{A})$ be the

structure whose domain of discourse is A, in which $t(x,y)$ is interpreted as $h \cdot x + k \cdot y$. This is a group only in the trivial case in which it reduces to the additive group of the ring:

LEMMA 2.2. *If $\mathcal{R}(h,k,\mathcal{A})$ is a group of exponent n, then $h = k = 1$ and $n = 0$ in $\mathcal{A}$.*

PROOF. Assume it is a group of exponent n. Let us use x^i to denote the i-fold t product (not the ring product), so, for example, $x^2 = hx + kx$; but $0, 1$ continue to denote the *ring*'s 0 and 1. By induction on i, $0^i = 0$ for all i; then, since x^n is the group identity, and hence, independent of x, we have $x^n = 0^n = 0$ for all x (so the group identity is in fact 0). Using $t(y, x^n) = t(x^n, y) = y$, we may set $y = 1$ to get $h = k = 1$. So, $t(x,y) = x + y$, whence $0 = x^n = nx$; taking $x = 1$, we have $n = 0$. ∎

We now consider how to implement Lemma 2.2 to eliminate many $(\alpha = x)$ as candidates for single axioms for groups of exponent 4. We do not know whether the existence of nongroup ring models for $(\alpha = x)$ is decidable, but the existence of such a model built from a commutative ring is decidable as follows. Say we consider α containing x, y, z. We may consider h, k as unknowns, replace each $t(\gamma, \delta)$ by $h \cdot \gamma + k \cdot \delta$ in the expression $\alpha - x = 0$, and then use the coefficients of x, y, z to obtain three polynomial equations: $P_x(h,k) = 0$, $P_y(h,k) = 0$, $P_z(h,k) = 0$. Let $\mathbb{Z}(h,k)$ be the ring of polynomials over $\mathbb{Z}$ in two variables h, k, and let $\mathcal{I}$ be the ideal in $\mathbb{Z}(h,k)$ generated by h, k. Then the following are equivalent:

1. In every commutative ring, $P_x(h,k) = P_y(h,k) = P_z(h,k) = 0$ implies that $h = k = 1$ and $4 = 0$.
2. $\mathcal{I}$ contains the polynomials $h - 1$, $k - 1$, and 4.

One may thus determine the existence of a nongroup commutative-ring model by implementing a general algorithm for deciding membership of polynomials in finitely generated ideals in $\mathbb{Z}(h,k)$.

However, for the purpose of this paper, we found it easier to implement a simpler and more specific test on our candidate $(\alpha = x)$. As a preliminary pass, we checked the equations for each candidate in $\mathbb{Z}_p$ for small values of p (from 3 to 13), running through all possible values of h, k except $h = k = 1$. We found in our search that this eliminated most of the α. For the few that were left, it was fairly easy to solve the equations by hand, and in fact the models obtained were built from fields, simplifying the algebra. The following three examples illustrate the method.

For the first example, consider $(\alpha = x)$, where α is

$$t(t(y,y), t(y, t(t(y, t(x,z)), t(z, t(z,z))))).$$

If, in $(\alpha = x)$, we replace $t(x,y)$ by $h \cdot x + k \cdot y$, and expand, and then equate the coefficients of x, y, z, we get the three equations, $kkhkh = 1$, $hh + hk + kh + kkhh = 0$, and $kkhkk + kkkh + kkkkh + kkkkk = 0$. In a field, the first equation is simply $h^2k^3 = 1$; if $v = hk$, then $h = v^3$ and $k = v^{-2}$. Putting in these values for h, k in terms of v automatically solves the first equation, and the next two reduce to $f(v) = 0$ and $g(v) = 0$, where $f(v) = v^5 + v + 2$ and $g(v) = v^7 + 2v^5 + 1$. Of course, these have the common solution $v = 1$ in a field of characteristic 2, which corresponds to the model $\mathcal{R}(1, 1, \mathbb{Z}_2)$, which is a group, but we wish to see whether any other solution exists. The Euclidean algorithm, applied in the field of rationals, computes a greatest common divisor, $h(v)$, along with polynomials $a(v)$ and $b(v)$ such that $h(v) = a(v) \cdot f(v) + b(v) \cdot g(v)$. If $h(v)$ is not a constant, then we are done; we may simply take a root in the complex numbers. If $h(v)$ is a constant, as is the case in this particular example, then the polynomials f and g are relatively prime over the rationals, and thus have no common root in any field of characteristic 0. However, now multiplying through by some integer, we obtain $\hat{h} = \hat{a}(v) \cdot f(v) + \hat{b}(v) \cdot g(v)$; here, $\hat{h}$ is an integer and $\hat{a}$ and $\hat{b}$ are polynomials with integer coefficients. Then the polynomials can only have common solutions in a field of characteristic p where p is a prime divisor of $\hat{h}$, and a complete description of these solutions can be obtained by applying the Euclidean algorithm in $\mathbb{Z}_p$. In the particular case in hand, we find a common solution, $v = 19$ in $\mathbb{Z}_{103}$, whence $h = 61$ and $k = 2$.

For the second example, consider $(\alpha = x)$, where α is

$$t(y, t(t(y, y), t(t(y, t(x, z)), t(z, t(z, z))))).$$

The three equations obtained now are $kkhkh = 1$, $h + khh + khk + kkhh = 0$, and $kkhkk + kkkh + kkkkh + kkkkk = 0$. Again, in a field, the first equation is $h^2k^3 = 1$, and we follow the same procedure, but now $f(v) = v^5 + v^4 + v^3 + 1$ and $g(v) = v^7 + 2v^5 + 1$. The Euclidean algorithm shows that f, g are relatively prime in every field except for fields of characteristic 2, in which the greatest common divisor is $v^4 + v^2 + v + 1 = (v + 1)(v^3 + v^2 + 1)$. As explained above, we discard the root $v = -1 = 1$. The polynomial $v^3 + v^2 + 1$ is irreducible over $\mathbb{Z}_2$, but adjoining a root, c, of this, we move to $GF(8)$, where $h = c^3 = c^2 + 1$ and $k = c^{-2} = c + 1$.

The third example shows that it is not true in general that the existence of a ring model implies that the ring may be taken to be a field. Consider $(\alpha = x)$, where α is

$$t(y, t(t(y, t(y, t(y, t(x, z)))), t(t(z, z), z))).$$

The three equations obtained now are $khkkkh = 1$, $h + khh + khkh + khkkh = 0$, and $khkkkk + kkhh + kkhk + kkk = 0$. In any commutative ring, these are equivalent to $h^2k^4 = 1$, $1 + hk + hk^2 + hk^3 = 0$, and $hk^3 + h^2 + hk + k = 0$. These have the solution $h = k = 5$ in $\mathbb{Z}_8$. However, in a field, the first equation implies that $h = \pm k^{-2}$; then, the next two equations imply that the field has characteristic 2 and $h = k = 1$. Actually, since $8 \leq 13$, this particular $(\alpha = x)$ was eliminated by our preliminary pass, which searched through all h, k for $\mathbb{Z}_8$.

Finally, we turn to models constructed by a special case of the Knuth-Bendix [8] method. Suppose that α is any term written with a binary t and variables. Call α *free* iff whenever β is a subterm of α other than a variable or α itself, and β' is a renaming of β with distinct variables, then α and β' are not unifiable. For example, $t(x, y)$ and $t(x, t(x, x))$ are free, but $t(y, t(x, y))$ is not, since it is unifiable with $t(x1, y1)$.

Now if α is free, then $(\alpha = x)$ cannot imply the associative law except in a few trivial cases, such as when α is $t(x, y)$.

LEMMA 2.3. *If α is free and contains the variable x, and $V(\alpha) \geq 3$, then there is a nonassociative model for $(\alpha = x)$.*

PROOF. Let A be the set of all ground terms formed by using t and constants a, b, c. If $\delta \in A$, call δ *reduced* iff it cannot be demodulated with $(\alpha = x)$. For any $\delta \in A$, we may demodulate δ with $(\alpha = x)$ until we obtain a reduced term, and, since α is free and contains x, any sequence of these demodulations will result in the same term, which we call $\mathrm{red}(\delta)$. Let B be the set of all reduced terms in A. On B, we may define the product of two terms γ and δ to be the term be $\mathrm{red}(t(\gamma, \delta))$, and verify that this is a model for $(\alpha = x)$. By $V(\alpha) \geq 3$, $\mathrm{red}(t(a, t(b, c)))$ cannot be the same as $\mathrm{red}(t(t(a, b), c))$, so associativity fails. ∎

The Knuth-Bendix method could be automated as part of a search, but we did not actually do so, since it was needed only to refute the two equations:

A3. $t(y, t(t(y, y), t(t(y, t(x, t(z, t(z, z)))), z))) = x$,

A4. $t(y, t(t(t(t(y, y), y), t(t(x, t(z, z)), z)), z)) = x$.

The α in both these are free, as can easily be verified, either by hand or with the aid of OTTER.

3. EASY RESTRICTIONS

Throughout this section, n denotes an integer greater than 1. We describe some syntactic restrictions on α if $(\alpha = x)$ is to be a single axiom for groups of exponent n.

LEMMA 3.1. *If $(\alpha = x)$ is valid in all groups of exponent n, then x occurs $kn + 1$ times in α for some integer k, and for every variable y other than x, y occurs kn times in α for some integer k (depending on y).*

PROOF. Otherwise, $(\alpha = x)$ would not be valid in the additive group $\mathbb{Z}_n$. ∎

Since all groups of exponent 2 are Abelian, the condition of Lemma 3.1 is sufficient as well as necessary for $n = 2$. Thus, for example, $(yxzyz = x)$ is valid in all groups of exponent 2. However, although $(yyyxy = x)$ satisfies the condition of Lemma 3.1 for $n = 4$, it is valid in only the Abelian groups of exponent 4, and not all groups of exponent 4 are Abelian. Similarly, $(yyxyy = x)$ is valid in all Abelian groups of exponent 4, as well as some (for example, the quaternion group), but not all (see below), non-Abelian ones.

LEMMA 3.2. *If $n \geq 3$, $0 < i < n$, and $j = n - i$, then there is a group of exponent n in which the equation $(y^i x y^j = x)$ is not valid.*

PROOF. This is equivalent to saying that if $n \geq 3$ and i is not divisible by n, then there is a group G of exponent n and an $a \in G$ such that a^i is not in the center of G. We begin with a few observations showing that it is sufficient to produce examples in a few special cases.

First, it is enough to consider the case where $i \mid n$, because in general, if $j = \gcd(i, n)$, then $j \mid n$. Say we produce a G of exponent n and an $a \in G$ with a^j not in the center. If $j = si + tn$, and $b = a^s$, then $b^i = a^j$, so we have an example for n, i as well. Now, it is enough to consider the case where $i = n/p$ for some prime p, because, in general, if $i \mid n$, we may choose p such that $i \mid (n/p)$; say $n/p = ri$. If we get G with $a^{n/p}$ not in the center and $b = a^r$, then $b^i = a^{n/p}$.

Next, if n is the least integer for which the lemma fails for some i, then for *every* prime factor q of n, either $n/q \leq 2$ or $(n/q) \mid i$. Otherwise, the lemma applied to n/q would say that there is a group of exponent n/q (and hence, of exponent n) containing an a with a^i not in the center. But now, we have just seen that we may assume that $i = n/p$ for some prime p. In this case, if q is any prime factor of n other than p, then n/q cannot divide i, so we have $p \leq n/q \leq 2$, so $p = n/q = 2$, so $n = 2q$. Of course, it is possible that p is the only prime factor of n. So, we have only two cases to consider: either $n = 2q$ and $i = q$ for some prime $q > 2$ or $n = p^k$ and $i = p^{k-1}$ for some prime p (possibly equal to 2).

In both cases, we may obtain G as a sub-direct product, of the form $G = \mathbb{Z}_r \times_\sigma H$, where $r \mid n$, H is an Abelian group of exponent n, and σ is an automorphism of H with σ^r the identity; we write both $\mathbb{Z}_r$ and H as additive groups, and the product operation on $\mathbb{Z}_r \times_\sigma H$ is then defined by

$$(s, x) \cdot (t, y) = (s + t, x + \sigma^s(y)).$$

A sufficient condition that G has exponent n is that whenever $x \in H$ and s is any integer,

$$\sum_{\mu<n} \sigma^{s\mu}(x) = 0. \qquad (*)$$

Furthermore, it is sufficient to verify $(*)$ when $0 < s < r$ and $s \mid r$; if $s = 0$, $(*)$ simply says that $n \cdot x = 0$, which is true in H, and if $s > 0$, $(*)$ follows from $(*)$ applied to $\gcd(s, r)$. To satisfy the lemma, we need also that σ^i is not the identity automorphism, so that $(1, 0)^i = (i, 0)$ is not in the center.

Now, in the case where $n = 2q$ and $i = q$ for some prime $q > 2$, we let $G = \mathbb{Z}_2 \times_\sigma \mathbb{Z}_q$, where $\sigma(x) = -x$. Then $\sigma^i = \sigma$ is not the identity (since $i = q$ is odd), and the only case for which $(*)$ needs to be verified is $s = 1$, where it is easy.

In the case that $n = p^k$ and $i = p^{k-1}$ for some prime p, we let $G = \mathbb{Z}_n \times_\sigma H$, where $H = \{x \in (\mathbb{Z}_p)^n : \sum x = 0\}$; here elements $x \in (\mathbb{Z}_p)^n$ are sequences of n elements of $\mathbb{Z}_p$, $\sum x$ denotes the sum of these elements (mod p), and σ is cyclic permutation: $\sigma(x_0, \ldots, x_{n-1}) = (x_1, \ldots, x_{n-1}, x_0)$. We must verify $(*)$ for $s = p^j$ and $0 \leq j < k$; but for $j = 0, s = 1$, this follows from the definition of H, and for $j > 0$, it follows from the fact that H has exponent p. Finally, we need an x such that $\sigma^i(x) \neq x$. Since $n > 2$, fix $\ell < n$ such that $\ell \neq 0, i$; let $x_0 = 1$ and $x_i = 0$ (so that $\sigma^i(x) \neq x$); let $x_\ell = -1$ and let $x_j = 0$ for all $j \neq 0, i, \ell$ (so that $x \in H$). ∎

PROOF OF THEOREM 1.1. For *a:* By Lemma 3.1, $V(\alpha) = kn + 1$, and $k = 0$ is obviously impossible. We show that $k = 1$ is also impossible. Note that x cannot be the left-most variable in α, since otherwise $(\alpha = x)$ would be valid in every model for $(t(x, y) = x)$. Likewise, x cannot be the right-most variable in α. Thus, if $k = 1$, then α is of the form $y^i x y^j$, where $0 < i < n$, and $j = n - i$. But then, by Lemma 3.2, the equation $(\alpha = x)$ would not be valid in all groups of exponent n unless $n = 2$. But if $n = 2$ (or is any other even number), then every Boolean group is of exponent n, so by Theorem 2.1, if $(\alpha = x)$ is valid in all groups of exponent n, it must be valid in some nongroup as well.

For *b:* By the above argument, plus Lemma 3.1, we see that for some variables y, z other than x, α must contain 1 occurrence of x and n occurrences each of y and z. Say the left-most variable of α is y. If some occurrence of y is to the right of the x in α, then, by Lemma 3.2 (letting z be the identity), we see that $(\alpha = x)$ would fail to be valid in some group of exponent n. So, all occurrences of y are to the left of x. Likewise, all occurrences of z are to the right of x, so $RA(\alpha)$ is $y^n x z^n$. ∎

For $n = 2$, Theorem 1.1(b) is false, since

$$((((y \cdot x) \cdot z) \cdot (y \cdot z)) = x)$$

is a single axiom for Boolean groups, found by Meredith and Prior [4] (see p. 221; they use 'E' for '$\cdot$'); others like this were found by McCune [6]. In fact, by the method of Section 5, for *no* α with $RA(\alpha)$ of the form $y^2 x z^2$ is $(\alpha = x)$ a single axiom for Boolean groups; even without a computer, one may easily verify that any such $(\alpha = x)$ will be valid in either the model described in Theorem 2.1 or the model $\mathcal{R}(2, 2, \mathbb{Z}_5)$ (see Section 2).

4. VERIFYING A SINGLE AXIOM

Suppose that $RA(\alpha)$ is $y^n x z^n$. Then $(\alpha = x)$ is clearly valid in all groups of exponent n, so to see that it is a single axiom, we should verify that it implies equations `G1`,`G2`,`G3` in Section 1. But in fact, `G1` (associativity) is sufficient.

LEMMA 4.1. *If $RA(\alpha)$ is $y^n x z^n$ and $(\alpha = x)$ implies the associative law, then $(\alpha = x)$ is a single axiom for groups of exponent n.*

PROOF. We have

$$x^n = x^n \cdot x^n \cdot \left(y^2\right)^n = \left(x^2\right)^n \cdot y^n \cdot y^n = y^n,$$

which yields `G2`, and

$$x y^n = x^n \cdot x y^n \cdot y^n = x^n \cdot x \cdot \left(y^2\right)^n = x,$$

which yields `G3`. ∎

Theorem 1.2 claimed that

`A0`. $t(y, t(t(y, t(t(y, y), t(x, z))), t(z, t(z, z)))) = x$

is a single axiom for groups of exponent 4. This can be proved using OTTER, but the proof seems a bit more difficult than similar verifications in earlier work along this line [5–7]. If we just run with axiom `A0` in the `sos`, we get a few other equations of the same length as `A0` (see below), but nothing shorter. However, `A0` may easily be verified by a sequence of four short OTTER runs, as we describe now.

A binary function is called *right cancellative* iff it satisfies the axiom

$$t(y, x) = t(z, x) \Rightarrow \; y = z$$

and *left cancellative* iff it satisfies the axiom

$$t(x, y) = t(x, z) \Rightarrow \; y = z.$$

The function is called *cancellative* iff it is both left and right cancellative. Our proof involves establishing as a lemma that t is cancellative. Once cancellativity is established, we can express it in OTTER by putting the four clauses

```
-(t(y,x) = t(z,x)) | (y = z).
-(t(x,y) = t(x,z)) | (y = z).
-(t(y,x) = u) | -(t(z,x) = u) | (y = z).
-(t(x,y) = u) | -(t(x,z) = u) | (y = z).
```

into the `usable` list. We set `ur_res` so that these clauses can be used to derive new equations. Logically, the last two clauses are equivalent to the first two, but it is sometimes useful to include them because if α and β are long terms, and γ and δ are short terms, then once we have $(t(\alpha,\gamma)=\delta)$ and $(t(\beta,\gamma)=\delta)$, we can derive $(\alpha=\beta)$ without having to first construct the longer intermediary $(t(\alpha,\gamma)=t(\beta,\gamma))$.

When using cancellativity, we set the two OTTER switches `para_into_units_only` and `para_from_units_only` so that we do not generate any nonunit clauses in the search. On all runs, we set `para_into`, `para_from`, `order_eq`, `dynamic_demod`, and `back_demod`. The weight limit is probably not very important here; we set the `max_weight` to 40 and the `pick_given_ratio` to 3. The axiom `A0` was always in the `sos` and the `demodulator` list and `(x = x)` was in the `usable` list. We describe the four runs below, which were done on OTTER version 2.2xa, giving the run time on a DECstation 5000, and the clause number at which a unit conflict was found.

1. Prove right cancellativity by adding `(t(b,a) = t(c,a))` and `(b != c)` in the `sos`. Unit conflict at 0.07 seconds, clause number 10. Note that right cancellativity is really trivial because of the $t(x,z)$ in `A0`.
2. Prove left cancellativity by adding `(t(a,b) = t(a,c))` and `(b != c)` in the `sos`. Unit conflict at 1.08 seconds, clause number 33.

In the next two runs, the four clauses expressing cancellativity were added to the `usable` list.

3. Prove that $\exists x(t(x,x)=x)$ (an idempotent exists) by adding `(t(x,x) != x)` into the `sos`. Unit conflict at 4.48 seconds, clause number 252.
4. Prove the associative law by adding `(t(a,t(b,c)) != t(t(a,b),c))` into the `sos`. We called the idempotent e and added `(t(e,e) = e)` into the `sos` and demodulators. For this run only, we decreased the `max_weight` to 20. Unit conflict at 93.11 seconds, clause number 405. Now, by Lemma 4.1, we are done.

Running with just equation `A0` in the sos, we very quickly produce four other equations of the same size:

`B1`. $t(t(z,t(t(z,z),t(t(z,x),y))),t(y,t(y,y)))=x$,
`B2`. $t(t(z,z),t(t(z,t(t(z,x),t(y,t(y,y)))),y))=x$,
`A3`. $t(y,t(t(y,y),t(t(y,t(x,t(z,t(z,z)))),z)))=x$,
`B4`. $t(t(z,t(t(z,t(t(z,z),x)),t(y,t(y,y)))),y)=x$.

These equations, or their mirrors, also turned up in the search described in Section 5. It is natural to ask whether they are also single axioms.

Now `B1` and `B2` are also single group axioms—the easiest way to verify this on OTTER is to show that they imply `A0`. `A3` and `B4` are not, as explained in Section 2, where `A3` and `A4` (the mirror of `B4`) were given as examples of Lemma 2.3.

PROOF OF THEOREM 1.2. We have just verified `A0`,`B1`,`B2`, and `A1`,`A2` are the mirrors of `B1`,`B2`. ∎

One can also see, without OTTER, that the axioms `A0`,`B1`,`B2`,`A3`,`B4` are all equivalent under cancellativity. This is explained at the end of Section 5.

5. THE EXPONENT 4 SEARCH

We prove Theorem 1.3 by searching through all associative variants of y^4xz^4. This search is similar in spirit to the ones described in [7].

We can figure out ahead of time how many terms to expect in such a search. Let c_n be the number of ways to associate a product of n factors. So, for example, $c_4 = 5$, since $wxyz$ can be associated in the five ways:

$$w((xy)z), \qquad w(x(yz)), \qquad (wx)(yz), \qquad ((wx)y)z, \qquad (w(xy))z.$$

These are the Catalan numbers (see, e.g., [9]), and may be computed either by the closed form,

$$c_n = \frac{(2n-2)!}{n!(n-1)!},$$

or by the recurrence:

$$c_1 = 1; \quad c_n = \sum_{i=1}^{n-1} c_i c_{n-i}, \qquad n > 1.$$

In particular, the value relevant here, c_9, is 1430.

We may immediately cut the 1430 candidates in half, to 715, by using mirror symmetry, as did McCune and Wos [5,6].

PROOF OF THEOREM 1.3. First, form a file consisting of all 1430 α such that $RA(\alpha)$ is y^4xz^4; this can easily be done with the aid of OTTER. Since x occurs exactly once in α, we can implement mirroring by keeping in this file only the 715 α that have a subterm of the form $t(x, \delta)$, and deleting the 715 with a subterm of the form $t(\delta, x)$.

Next, we can delete from the 715 all those α such that α can be demodulated to x using two-variable equations true in all Boolean groups, as described in Section 2; 169 remain.

Then, as described in Section 2, we can delete from these 169 all α such that $(\alpha = x)$ is valid in a ring model of the form $\mathcal{R}(h, k, \mathbb{Z}_p)$, where p is member of the list [3,5,7,8,23,103]. This was done with the aid of a Prolog program which reads terms from a file and, for each term, looks through all p on a given list of integers and all $h, k < p$. The actual list used was obtained by some preliminary hacking. We first ran it with the list of all integers between 3 and 13. The number of survivors was small enough that we could look through their equations by hand, as explained in Section 2, to see which values of p should to be added to the list. We also removed from the list those values of p which were not used.

After these deletions, only 10 candidates remain. These are the equations A0–A9 listed below. We have also listed their mirrors, B0–B9.

A0. $t(y, t(t(y, t(t(y, y), t(x, z))), t(z, t(z, z)))) = x,$

B0. $t(t(t(t(z, z), z), t(t(t(z, x), t(y, y)), y)), y) = x,$

A1. $t(t(t(y, y), y), t(t(t(y, t(x, z)), t(z, z)), z)) = x,$

B1. $t(t(z, t(t(z, z), t(t(z, x), y))), t(y, t(y, y))) = x,$

A2. $t(t(y, t(t(t(t(y, y), y), t(x, z)), z)), t(z, z)) = x,$

B2. $t(t(z, z), t(t(z, t(t(z, x), t(y, t(y, y)))), y)) = x,$

A3. $t(y, t(t(y, y), t(t(y, t(x, t(z, t(z, z)))), z))) = x,$

B3. $t(t(t(z, t(t(t(t(z, z), z), x), y)), t(y, y)), y) = x,$

A4. $t(y, t(t(t(t(y, y), y), t(t(x, t(z, z)), z)), z)) = x,$

B4. $t(t(z, t(t(z, t(t(z, z), x)), t(y, t(y, y)))), y) = x,$

A5. $t(y, t(t(y, y), t(t(y, t(x, z)), t(z, t(z, z))))) = x,$

B5. $t(t(t(t(t(z, z), z), t(t(z, x), y)), t(y, y)), y) = x,$

A6. $t(t(t(t(y, y), y), t(t(y, t(x, z)), z)), t(z, z)) = x,$

B6. $t(t(z, z), t(t(z, t(t(z, x), y)), t(y, t(y, y)))) = x,$

A7. $t(t(t(y, y), y), t(t(y, t(t(x, t(z, z)), z)), z)) = x,$

B7. $t(t(z, t(t(z, t(t(z, z), x)), y)), t(y, t(y, y))) = x,$

A8. $t(y, t(t(y, t(t(y, y), t(x, t(z, t(z, z)))))), z)) = x,$

B8. $t(t(z, t(t(t(t(t(z, z), z), x), t(y, y)), y)), y) = x,$

A9. $t(y, t(t(t(t(t(y, y), y), t(x, z)), t(z, z)), z)) = x,$

B9. $t(t(z, t(t(z, z), t(t(z, x), t(y, t(y, y))))), y) = x.$

Now, A0,A1,A2 are indeed single axioms, by Theorem 1.2. A3 and A4 fail to be single axioms by the Knuth-Bendix method; see Lemma 2.3 and the following discussion.

A5 is not a single axiom, since, as we showed in Section 2, it has a ring model using $GF(8)$. One may verify that the same ring model, possibly interchanging the values of h, k, will also satisfy all of A5–A9 and B5–B9, or, one may use OTTER and avoid the algebra as follows. If one runs OTTER with A5, plus cancellativity, as explained in Section 4, one soon derives equations B6,B7,A8,B9. Since cancellativity holds in the ring model, this implies that the same model satisfies B6,B7,A8,B9, so these equations, and their mirrors, fail to be single axioms.

Now, only A0,A1,A2 and their mirrors remain. ∎

The above discussion seems to indicate that the 20 equations, A0–A9 and B0–B9, fall into 4 sets of 5. This can be explained without using OTTER, and involves another symmetry that, if applied in our search, would have reduced the original file of candidates to length 164.

If $RA(\alpha)$ is $y^n x z^n$, where $n > 0$, we define the term $\mathcal{T}(\alpha)$ as follows: Let β, γ be the (unique) terms such that β contains x and γ does not, and α is either of the form $t(\beta, \gamma)$, or of the form $t(\gamma, \beta)$. Write β as $\beta(x, y, z)$. If α is $t(\beta, \gamma)$, then $\mathcal{T}(\alpha)$ is $\beta(t(x, \gamma), y, z)$. If α is $t(\gamma, \beta)$ then $\mathcal{T}(\alpha)$ is $\beta(t(\gamma, x), y, z)$. For example, if α is the left-hand side of A1,

$$t(\mathbf{t}(\mathbf{t}(\mathbf{y}, \mathbf{y}), \mathbf{y}), \quad t(t(t(y, t(x, z)), t(z, z)), z)),$$

then $\mathcal{T}(\alpha)$ is

$$t(t(t(y, t(t(\mathbf{t}(\mathbf{t}(\mathbf{y}, \mathbf{y}), \mathbf{y}), x), z)), t(z, z)), z),$$

which is the left-hand side of B3 (if we interchange y/z). Applying $\mathcal{T}$ again, we get the left-hand side of A2. If $\mathcal{S}$ is the set of all α such that $RA(\alpha)$ is $y^n x z^n$, then $\mathcal{T}$ is a 1-1 map from $\mathcal{S}$ into $\mathcal{S}$, and therefore, breaks up $\mathcal{S}$ into cycles. Four such cycles are A0,B1,A3,B2,B4 and A5,B6,B7,A8,B9, and their mirrors, B0,A1,B3,A2,A4 and B5,A6,A7,B8,A9. Cycles can have various lengths, and some of them equal their own mirrors. For example, in the cycle

$$t(t(t(y, y), y), t(y, t(t(x, z), t(z, t(z, z))))),$$
$$t(y, t(t(t(t(t(y, y), y), x), z), t(z, t(z, z)))),$$
$$t(t(t(t(t(y, y), y), t(y, x)), z), t(z, t(z, z))),$$
$$t(t(t(t(y, y), y), t(y, t(x, t(z, t(z, z))))), z),$$

the first and the third are mirrors of each other (interchanging y/z as before), and the second and fourth are mirrors of each other.

Under the additional assumption of cancellativity, $(\alpha = x)$ implies $(\mathcal{T}(\alpha) = x)$. For example, if α is $t(\beta(x, y, z), \gamma)$ then

$$(\alpha = x) \Rightarrow \ (t(\beta(t(x, \gamma), y, z), \gamma) = t(x, \gamma)) \Rightarrow \ (\beta(t(x, \gamma), y, z) = x)$$

by right cancellation. Thus, under cancellativity, all members of a cycle are equivalent. So, if we have proved $(\alpha = x)$ is not a single axiom using a model satisfying cancellativity, we have also refuted all members of the cycle of α, and their mirrors. For example, all the ring models satisfy cancellativity, so once we refuted A5 using $GF(8)$, we have immediately refuted A5–A9 and B5–B9. Likewise, the model described in the proof of Theorem 2.1 satisfies cancellativity. However, the Knuth-Bendix models do not. In the cycle A0,B1,A3,B2,B4, we refuted A3 and B4 Knuth-Bendix models, while A0, B1, and B2 are single axioms for groups of exponent 4.

One can break up the original 1430 candidates for the exponent 4 search into equivalence classes, where each class is a cycle plus its mirror (which is either the same as or disjoint from the cycle). There are 164 such classes. There are, respectively, 7,6,4,2 cycles of lengths 2,4,6,8 that are the same as their mirrors, contributing $7 \cdot 2 + 6 \cdot 4 + 4 \cdot 6 + 2 \cdot 8 = 78$ terms. And, there

are, respectively, 10,26,31,35,25,15,3 pairs of cycles of lengths 2,3,4,5,6,7,8 that are disjoint from their mirrors, contributing $2\cdot(10\cdot 2+26\cdot 3+31\cdot 4+35\cdot 5+25\cdot 6+15\cdot 7+3\cdot 8)=1352$ terms. This accounts for all $1430=78+1352$ terms. The search could have been organized by choosing one representative of each equivalence class and trying to refute it by a model satisfying cancellativity. This would have eliminated all representatives except A0.

6. NEUMANN'S SINGLE AXIOM

If one is concerned just with the existence of single axioms, rather than their size, then Theorem 3 of Neumann [3] is much more general than the results presented here. He considered inverse (i) and product as basic symbols and showed that if δ is any term in product and inverse, the variety of all groups in which δ is the identity can be axiomatized by the single axiom $(\alpha = x)$, where α is

$$u\cdot i\Big(\Big((i(i(y)(i(u)x))\cdot z)\cdot i(yz)\Big)\cdot i(\delta\cdot i(\delta'))\Big).$$

Here, x, y, z, u are variables that do not occur in δ, and δ' denotes a renaming of δ using new variables. In particular, to axiomatize groups of exponent n, we may take δ to be w^n. To get a term in product only, we may replace each $i(\beta)$ by β^{n-1}. Then, $V(i(\beta))=(n-1)V(\beta)$, from which we easily compute $V(\alpha)=n^4-2n^2+n+1$.

With the aid of OTTER, one can verify Neumann's result as follows. First, it is easy to see (even by hand) that $(\alpha = x)$ is valid in all groups in which δ is the identity. The main difficulty is to see that every model for $(\alpha = x)$ is a group. Once this is done, then (even by hand) we can see that every model for $(\alpha = x)$ satisfies $(\delta = \delta')$; then, fixing all the variables in δ' to be the identity, we get that δ is the identity in these models.

To prove that every model for $(\alpha = x)$ is a group, we may proceed as follows. Let β be the term obtained from α by replacing both δ and δ' by the constant d. Note that every model for $(\alpha = x)$ may be considered to be a model for $(\beta = x)$, since we may fix all the variables occurring in δ and δ' to be the same object. We now do a sequence of three OTTER runs. On the first run, we derive $t(i(x),t(x,y))=t(i(z),t(z,y))$ from $(\beta = x)$, which means that the value of $t(i(x),t(x,y))$ depends only on y; call this $h(y)$. Then, on the second run, we can add in $(t(i(x),t(x,y))=h(y))$ and derive $(t(i(h(x)),x)=t(i(h(y)),y))$, which means that $t(i(h(y)),y)$ is a constant; call it e. On the third run, we may forget about h and simply add in $(t(i(t(i(x),t(x,y))),y)=e)$; from this we derive $t(x,e)=x$, $t(x,i(x))=e$, and $t(t(y,z),u)=t(y,t(z,u))$. So, we have right identity, right inverse, and associativity.

There are schemata simpler than Neumann's that can be verified in the same way. One such is $(\alpha = x)$, where α is

$$\big(i(\delta\cdot z)\cdot y\big)\cdot i\big(i(\delta'\cdot(z\cdot x))\cdot y\big).$$

To verify this, just let OTTER run with

$$\big(i(d\cdot z)\cdot y\big)\cdot i\big(i(d\cdot(z\cdot x))\cdot y\big)=x. \tag{1}$$

The three equations $x\cdot(y\cdot i(y))=x$, $x\cdot i(x)=y\cdot i(y)$, and $(x\cdot y)\cdot z=x\cdot(y\cdot z)$ will soon appear, so every model for (1) is a group.

This method of verification also establishes that these schemata can be used in a more general way. Suppose that γ and δ are any terms in t, i and variables other than x, y, z such that γ and δ become the same when all their variables are replaced by the single variable u. Then we have actually shown that

$$\big(i(\gamma\cdot z)\cdot y\big)\cdot i\big(i(\delta\cdot(z\cdot x))\cdot y\big)=x \tag{2}$$

is a single axiom for the variety of groups satisfying the equation $\gamma=\delta$. For example, if we wish to axiomatize the variety of groups satisfying $u^2v^2=v^2u^2$, we can let γ be $(u\cdot(u\cdot(v\cdot v)))$ and δ be $(v\cdot(v\cdot(u\cdot u)))$, producing the single axiom

$$\big(i((u\cdot(u\cdot(v\cdot v)))\cdot z)\cdot y\big)\cdot i\big(i(v\cdot(v\cdot(u\cdot u)))\cdot(z\cdot x)\big)\cdot y)=x, \tag{3}$$

which is the shortest known single axiom for this variety. Actually, (3) is due to McCune, and we found (2) by reverse engineering, starting from (3).

7. SUMMARY

This paper suggests the following two avenues for future research. In mathematics, there remains the obvious question of whether our results extend to even exponents greater than 4. In automated reasoning, there is the question of whether one can automate some of the deduction steps. In the verifications of our single axioms for exponent 4 groups, and of Neumann's general scheme, we used multiple OTTER runs, with earlier runs verifying lemmas used by later runs. It would be of interest if the process of finding (and proving) the correct lemma could be automated.

REFERENCES

1. W.W. McCune, OTTER 2.0 Users Guide, Technical Report ANL-90/9, Argonne National Laboratory, Argonne, IL, (1990).
2. W.W. McCune, What's New in OTTER 2.2, Technical Memo ANL/MCS-TM-153, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, IL, (1991).
3. B.H. Neumann, Another single law for groups, *Bull. Australian Math. Soc.* **23**, 81–102 (1981).
4. C.A. Meredith and A.N. Prior, Equational logic, *Notre Dame J. Formal Logic* **9**, 212–226 (1968).
5. W.W. McCune and L. Wos, Applications of automated deduction to the search for single axioms for exponent groups, In *Logic Programming and Automated Reasoning*, pp. 131–136, Springer-Verlag, (1992).
6. W.W. McCune, Single axioms for groups and Abelian groups with various operations, *J. Automated Reasoning* **10**, 1–13 (1993).
7. K. Kunen, Single axioms for groups, *J. Automated Reasoning* **9**, 291–308 (1992).
8. D.E. Knuth and P.B. Bendix, Simple word problems in universal algebras, In *Computational Problems in Abstract Algebra*, (Edited by J. Leech), pp. 263–297, Pergamon Press, (1970).
9. R.A. Brualdi, *Introductory Combinatorics*, North-Holland, (1977).